Achieving Information Superiority

by Patricia Barwinczak

MUCH LIKE the printing press in the 17th century, computers have become the catalyst for economic, cultural and political change on a global scale. The global information environment (GIE) is characterized by the exponential growth of the microchip's computing power, the availability and affordability of high-speed information technologies and global computer network proliferation. The US military has been integrating advanced information technology (IT) into its operations and now it is almost totally dependent upon computers, computer networks and high-speed digital communications.

Despite governmentwide consensus that the information revolution is having a profound impact on our society, the Department of Defense (DOD) has not fully articulated this impact in a way that provides clear guidance for military planners. Terms such as *information warfare, information operations (IO) and information superiority* have been used in DOD directives to address the operational and strategic importance of information systems (INFOSYS), both human and technological. However, confusion persists over how these concepts will advance our national security interests and, most important for the military, what operational, technical and institutional requirements they necessitate.

This article posits that the global availability of sophisticated IT will lead to a condition of *sufficient equivalence* with respect to US and adversary intelligence, surveillance and reconnaissance (ISR), command and control (C^2) and force application capabilities. It further suggests that the United States will attempt to resist the use of lethal force by applying techniques to affect the enemy's INFOSYS to achieve a political-military advantage. This strategy may change the way we use, or even preclude the use of, traditional force elements by shifting the central focus of military strategy from force attrition to GIE competition for superiority in the military information environment (MIE) that enables the accomplishment of national security objectives.

Unconstrained availability—and ever-decreasing cost of highly sophisticated sensor and imaging technologies and advanced communications and computers—will make it possible for motivated adversaries to essentially "catch up" with the United States' ability to "see" the battlespace and C^4 ISR connectivity of command. Future effectiveness in warfare will be increasingly dependent on the relative capabilities of opponents to use advanced INFOSYS and efficient decision processes to effectively integrate . . . political-military functions.

Further, this article discusses how the information revolution is likely to affect our military power relative to future adversaries, and offers a basic construct for thinking about how IO will allow the military to gain and sustain an information advantage *vis-à-vis* future adversaries. The goal is to attain greater understanding of IO's potential military utility and how information superiority can change US defense operations and strategy.

The Information Revolution: National Security Implications

How will the US military protect its political and economic interests in a world that is being transformed by the information revolution? As other societies assimilate advanced IT into their commercial affairs, they will also integrate these technologies into their military forces and planning. Unconstrained availability—and ever-decreasing cost of highly sophisticated sensor and imaging technologies and advanced communications and comput-

ers—will make it possible for motivated adversaries to essentially "catch up" with the United States' ability to "see" the battlespace and command, control, communications and computer (C^4) ISR connectivity of command. Future effectiveness in warfare will be increasingly dependent on the relative capabilities of opponents to use advanced INFOSYS and efficient decision processes to effectively integrate the following political-military functions:

- Observe—collect relevant information and intelligence (RII).
- C^2—use collected information to make good situational/battlespace decisions and communicate those decisions to their forces.
- Execute—conduct missions in support of national/organizational objectives.
- Support—meet manpower, equipment and logistic mission needs.

More important, potential adversaries will develop *asymmetric* strategies to corrupt US INFOSYS in an attempt to circumvent our advantage in conventional force application.

Currently, the United States enjoys overall superiority in its conventional warfighting information architecture and force elements versus any potential adversary. However, given trends that can already be identified, the future international security environment is likely to challenge that superiority.

Decreasing US advantage in military RII. The United States will continue to increase its dependence on extremely rapid and interconnected INFOSYS—military and commercial—and to upgrade the MIE that supports its tactical capabilities. We must assume that some future adversaries already have access to militarily significant information technologies, such as navigation and high-resolution imagery, and to global media and computer networks. These mostly commercial-off-the-shelf (COTS) information assets could provide future enemies with their own clear battlespace view. Similarly, future competitors will be able to acquire and apply commercial IT to develop highly integrated and secure C^2 networks that thoroughly connect the command structure vertically and horizontally. Given the dual-use nature of information technologies, their contribution to advancing the military capabilities of future opponents cannot be limited or controlled by arms control agreements.

Many militarily critical information assets will reside in space or be airborne, and the competitor who controls the "high ground" will have a major strategic advantage. Threats to US space- and air-based platforms and sensors will be significant as countries develop antisatellite or precision surface-to-air weapons capable of destroying or disabling information-collection platforms. Weapon development or procurement is likely to be a key competitive strategy for potential adversaries.

The combination of decreasing cost and increasing quality of weapons available may give adversaries* sufficient equivalence *with respect to their ability to apply lethal force against US and allied interests. For example, a combination of integrated air defense systems, lethal and precise ballistic and cruise missiles and a small number of NBC weapons may prove extremely effective in preventing the United States from achieving its military objectives and potentially, due to the political consequences, from even engaging.

The US intelligence community has evidence that potential adversaries are pursuing strategies that focus on attacking and exploiting US INFOSYS. Computer network-based attacks will be a serious threat and future adversaries are likely to use computer network approaches to degrading US information advantages wherever and whenever possible.

Leveling the lethal playing field. The US advantage in precision-guided weapons, long-range and mobile advanced-strike platforms and stealth technology will significantly shrink in the next 25 years. Since the Cold War's end, proliferation of advanced weaponry has become a more serious threat as former Soviet militaries attempt to fend for themselves. Competitors are likely to focus their acquisition strategies on procuring longer-range ballistic missiles, stealthy cruise missiles with advanced guidance and target recognition technologies and weapons of mass destruction (WMD). Ballistic missiles are likely to be deployed on mobile ground-based platforms and sea-based systems. Sophisticated air defenses will be acquired to deter and combat US and allied air campaigns, but procurement of expensive high-tech fighter aircraft and strategic bombers will be a low priority.

As recent events have demonstrated, nonproliferation efforts will not keep advanced or nuclear, chemical and biological (NBC) weapons out of the hands of those countries that want them and can afford them. NBC warheads could be deployed on short-, medium- and long-range missiles. For instance, a few dozen NBC weapons could have as

much utility in a theater war as a few thousand current warheads. These weapons could also critically degrade C^2 because high electromagnetic pulse (EMP) burst weapons could degrade or destroy US space assets and ground-based electronic and power systems, causing a devastating impact.

A few future competitors will be able to acquire most of the advanced technology weaponry they need to challenge the United States in terms of weapons' range, lethality and precision as a peer or near-peer competitor. We can expect significant qualitative improvements to adversaries' military capabilities as they integrate commercial IT into their force structure. This will increase their effectiveness against US forces and afford the adversary an increased chance of success with fewer, but more powerful, weapons.

Future wars may center on attacking and defending information and INFOSYS as opposed to deploying lethal forces into regional theaters of operation. INFOSYS themselves will have become the most valuable military asset for modern societies, and protecting the integrity and availability of information will become so politically and economically important that threats to it may precipitate armed conflict.

The combination of decreasing cost and increasing quality of weapons available may give adversaries *sufficient equivalence* with respect to their ability to apply lethal force against US and allied interests. For example, a combination of integrated air defense systems, lethal and precise ballistic and cruise missiles and a small number of NBC weapons may prove extremely effective in preventing the United States from achieving its military objectives and potentially, due to the political consequences, from even engaging the enemy.

Increasing focus on INFOSYS. Despite the potential positive effects and greater understanding of foreign cultures and politics that global access and interactive media may bring, information globalization access will not negate the underlying reasons for conflict. Competition for resources or politicians intent on broadening their economic and political power bases will still precipitate crises and conflicts. Twenty to 30 years in the future, there will still be nation-states willing to go to war over threats to their economic, political and sociological structure. However, future wars may center on attacking and defending information and INFOSYS as opposed to deploying lethal forces into regional theaters of operation. INFOSYS themselves will have become the most valuable military asset for modern societies, and protecting the integrity and availability of information will become so politically and economically important that threats to it may precipitate armed conflict. For example, an information war could be precipitated by a dictator or non-state actor trying to control GIE access in an attempt to dominate the world's information sources. The theater of war could be global and may be fought on land, sea, air and space. Numerous scenarios could be postulated, with the competition focused on control and exploitation of information as the slogan "information is power" becomes applicable on a global scale.

Attacks on US INFOSYS via global networks have already occurred, and it has been extremely difficult to find the source of these attacks. Use of computer "hackers" and other nonlethal techniques for affecting information and INFOSYS are being used by military competitors because they are inexpensive and can achieve military objectives without provoking an overwhelming retaliatory response. Some competitors will employ highly mobile and lethal special forces armed with compact computer support to affect ground-based INFOSYS using specialized techniques. For those countries that cannot afford or decline the use of *sufficient equivalence* in conventional force structure with the United States, strategies afforded by information-age approaches to warfare may offer adversaries alternative means of "victory." In the future, the term "peer competitor" as it is understood today may be irrelevant to the outcome of conflict.

The trends described herein suggest three factors that converge to affect warfare's general conduct:

- Universal IT availability that could provide competitors with qualitatively similar ISR and C^2 capabilities.
- Acquisition of long-range, precision-strike weapons, NBC weapons and WMD providing for roughly equivalent force application capabilities.
- Development of strategies and capabilities aimed at affecting enemy information assets.

This last factor will become increasingly prevalent as the first two trends come to pass and sheer US firepower becomes less of a deterrent to potential adversaries. As future competitors level the playing field to compete with the United States with respect to their ability to observe and react to battlespace situations and force application capabilities—assuming

The days are long gone when the spread of information technology could be significantly slowed by the seizure of illegal exports in actions like this joint US-German operation in 1986 (*inset*). The problem is compounded by the ability of potential adversaries to acquire sophisticated weapon systems from countries with active arms industries. Below, one of the three Russian-built Kilo class submarines purchased by Iran passes through the English Channel.

US Naval Institute Proceedings, Inset: US Air Force

The US advantage in precision-guided weapons, long-range and mobile advanced-strike platforms and stealth technology will significantly shrink in the next 25 years. Since the Cold War's end, proliferation of advanced weaponry has become a more serious threat as former Soviet militaries attempt to fend for themselves. Competitors are likely to focus their acquisition strategies on procuring longer-range ballistic missiles, stealthy cruise missiles with advanced guidance and target recognition technologies and weapons of mass destruction. . . . Sophisticated air defenses will be acquired to deter and combat US and allied air campaigns.

they are successful at pulling those capabilities together into an integrated operational concept for employing forces—the cost of conventional mass destruction may be too high for either side to pay. The focus of US and adversarial targeting strategy will shift to INFOSYS and decision processes that support the effective use of these capabilities. In other words, the information enabling those capabilities becomes the focus of the competition.

The benefits of this shift in strategy are likely to be recognized sooner by those adversaries who choose not to compete with US conventional force capabilities. These competitors will be the first to develop offensive means to degrade our information advantage. Whether competing against a peer or a nonpeer adversary, the use of techniques to disrupt an adversary's INFOSYS and protect our own will shift the central focus of military strategy from force attrition to a competition for MIE superiority to attain national security objectives.

IO: Achieving Information Advantages

How does the US military plan to employ IO strategies in future conflict? The information revolution's impact on future military capabilities will be significant. As the military strategy target focus shifts to information resources that enable national power, IO—those actions that affect the enemy's information and INFOSYS (offensive IO), and protect friendly information and INFOSYS (defensive IO)—will begin to take on much greater importance. It is imperative that DOD articulate how IO relates to its larger goal of achieving an information advantage in future security environments.

A composite DOD definition of *information superiority* would be along the lines of "the ability to collect, process, synthesize and share vital information to a far-greater extent than an adversary can." This could include efforts to disrupt or exploit enemy systems. Information superiority should be understood as the dynamic relationship between adversary and friendly information capabilities and the respective offensive and defensive information operations affecting the applicable MIE that enables national security objectives to be accomplished. According to the *National Military Strategy 1997*, in the section titled "The Strategy—Shape, Respond, Prepare Now," information superiority "is not an

inherent quality but, like air superiority, must be achieved in the battlespace through offensive and defensive information operations."

Viewing information superiority as a dynamic state of affairs between adversaries allows it to be measured as a relative condition in which one side has a greater ability to influence or affect the MIE in support of its own national objectives. This condition could be fleeting or sustained throughout a conflict, and its geographic boundaries could be local, regional or global. Thinking about how IO can enable us to achieve a relative MIE advantage allows planners at all echelons to develop strategy and identify operational, organizational and technical requirements. By assessing our own—and a potential adversary's MIE—we can determine the offensive and defensive IO strategies that should be implemented to successfully influence or control any environment.

A full appreciation of one's own MIE, as well as the enemy's, and the offensive and defensive capabilities available for affecting that environment is required to determine what it will take to achieve information superiority in specific scenarios against specific adversaries. An enemy with an effective, survivable C^2 architecture and ISR system, minimal yet modern military forces and a clever strategy for exploiting US INFOSYS could challenge US warfighting superiority. We need to think "out of the box" about what IO can offer in terms of future competitive strategies.

The "information superiority" concept requires us to gain detailed intelligence on information target sets to develop an information order of battle. We need to know the adversary's INFOSYS and processes the same way we know the enemy's ground-, air- and sea-based force elements. Because the intelligence challenge is daunting, we must begin to take an organized communitywide approach to addressing this challenge. Friendly and adversary information target sets include, but may not be limited to, the following categories:

- Intelligence collection, transmission and fusion.
- Civilian decision makers and military commanders and their C^2 control links and facilities.
- INFOSYS that support force execution, weapon development and production, and force mobilization and support functions.

After gaining understanding of the friendly and adversary MIE, IO strategists and planners must determine inherent friendly INFOSYS vulnerabilities and assess the adversary's IO potential for attacking those vulnerabilities. They must concurrently understand which friendly capabilities are required to meaningfully influence, disrupt, deny or destroy an adversary's ability to gain information superiority.

A full appreciation of one's own MIE, as well as the enemy's, and the offensive and defensive capabilities available for affecting that environment is required to determine what it will take to achieve information superiority in specific scenarios against specific adversaries. An enemy with an effective, survivable C^2 architecture and ISR system, minimal yet modern military forces and a clever strategy for exploiting US INFOSYS could challenge US warfighting superiority. We need to think "out of the box" about what IO can offer in terms of future competitive strategies. Much work needs to be done to develop effective campaign plans focused on how to achieve an information advantage over future enemies.

This article posits that changes brought on by the information revolution may shift the central focus of political-military competitions from attrition and threat of attrition to strategies for gaining and sustaining a relative advantage over the strategic, operational and tactical information assets that enable the accomplishment of national security objectives. The term *information superiority* has become popular within DOD to emphasize the importance of developing our information and INFOSYS that have enabled the United States to have the most powerful military in the world. But information superiority must be understood as the result of offensive and defensive actions against the MIE of both adversaries. The United States must plan to counter adversary actions against its own MIE, and to execute IO against the high- and low-tech INFOSYS that will enable future adversaries to wage war against us. ***MR***

Patricia M. Barwinczak is a senior analyst at Science Applications International Corporation, McLean, Virginia. She received a B.A. from Cornell University and an M.S. from American University. She served as Net Assessment director, Office of the Secretary of Defense, and the Joint Staff and has held numerous positions in national security policy analysis, focusing on the revolution in military affairs and long-range planning issues, strategic nuclear doctrine, arms control and counterproliferation.